

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-274786

(43)Date of publication of application : 05.10.2001

(51)Int.Cl.

H04L 9/08

G06F 15/00

G09C 1/00

(21)Application number : 2000-051204

(71)Applicant : VICTOR CO OF JAPAN LTD

(22)Date of filing : 28.02.2000

(72)Inventor : KUROWA TOSHIO
SUGAWARA TAKAYUKI
IBA WATARU
UEDA KENJIRO
HIGURE SEIJI

(30)Priority

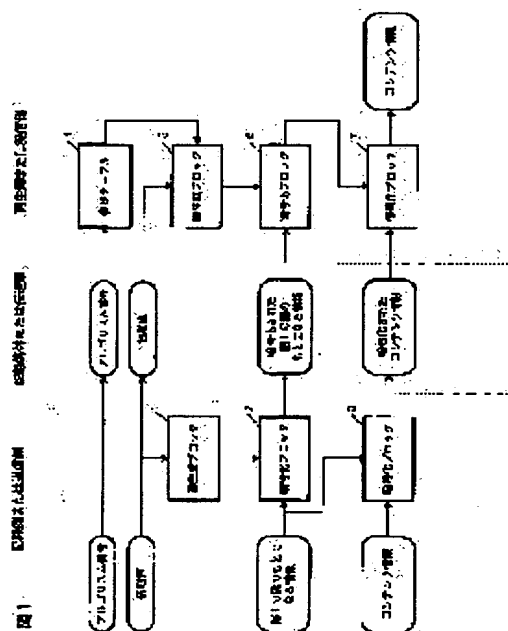
Priority number : 2000012733 Priority date : 21.01.2000 Priority country : JP

(54) CONTENTS INFORMATION TRANSMISSION METHOD, CONTENTS INFORMATION RECORDING METHOD, CONTENTS INFORMATION TRANSMITTER, CONTENTS INFORMATION RECORDER, TRANSMISSION MEDIUM AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a contents information transmission method, the recording method, transmitter, recorder, transmission medium and recording medium thereof, by which a decoder side cannot respectively identify key generating algorithms used for encryption according to each designated algorithm number only with the intelligence given to an encryption side, so as to more vigorously prevent unauthorized reproduction and copy of contents information, thereby enhancing copyright protection.

SOLUTION: The method adopts transmission or recording of encrypted contents information resulting from encrypting contents information, by using a 1st key generated from source information of the 1st key, source information of an encrypted 1st key resulting from encrypting source information of the 1st key, using a 2nd key generated by a prescribed key generating algorithm on the basis of a given initial value, algorithm identification information for identifying the prescribed by generating algorithm and initial value information denoting the initial value.



LEGAL STATUS

[Date of request for examination] 27.09.2002

[Date of sending the examiner's decision of rejection] 25.02.2005

BEST AVAILABLE COPY

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開 2001-274786

(P 2001-274786 A)

(43) 公開日 平成13年10月5日 (2001. 10. 5)

(51) Int. Cl. ⁷	識別記号	F I	テマコード* (参考)
H 0 4 L 9/08		G 0 6 F 15/00	3 3 0 Z 5B085
G 0 6 F 15/00	3 3 0	G 0 9 C 1/00	6 1 0 Z 5J104
G 0 9 C 1/00	6 1 0	H 0 4 L 9/00	6 0 1 A 9A001
			6 0 1 B

審査請求 未請求 請求項の数 1 4 O L

(全 8 頁)

(21) 出願番号 特願2000-51204 (P2000-51204)
(22) 出願日 平成12年2月28日 (2000. 2. 28)
(31) 優先権主張番号 特願2000-12733 (P2000-12733)
(32) 優先日 平成12年1月21日 (2000. 1. 21)
(33) 優先権主張国 日本 (J P)

(71) 出願人 000004329
日本ビクター株式会社
神奈川県横浜市神奈川区守屋町3丁目12番地
(72) 発明者 黒岩 俊夫
神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内
(72) 発明者 菅原 隆幸
神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内
(72) 発明者 猪羽 渉
神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

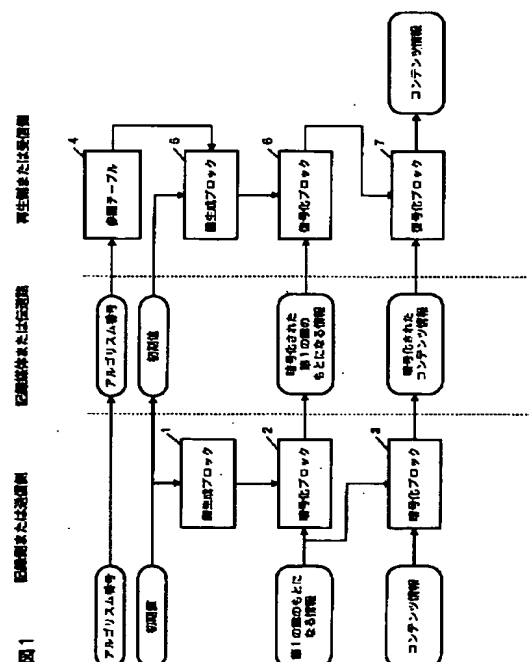
最終頁に続く

(54) 【発明の名称】 コンテンツ情報伝送方法、コンテンツ情報記録方法、コンテンツ情報伝送装置、コンテンツ情報記録装置、伝送媒体、及び記録媒体

(57) 【要約】

【課題】 暗号化側に与えられる知識のみでは、復号化側において、指定された各アルゴリズム番号に従って暗号化に用いた鍵生成アルゴリズムをそれぞれ特定できないようにすることにより、コンテンツ情報の不正な再生、コピーをより強力に防止し著作権保護の強化を可能とするコンテンツ情報伝送方法、記録方法、伝送装置、記録装置、伝送媒体、及び記録媒体を提供すること。

【解決手段】 第1の鍵のもとになる情報から生成された第1の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、与えられた初期値に基づき所定の鍵生成アルゴリズムにより生成された第2の鍵を用いて、前記第1の鍵のもとになる情報を暗号化した暗号化第1の鍵のもとになる情報と、前記所定の鍵生成アルゴリズムを特定するためのアルゴリズム特定情報と、前記初期値を示す初期値情報とを伝送または記録する。



【特許請求の範囲】

【請求項1】第1の鍵のもとになる情報から生成された第1の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

与えられた初期値に基づき所定の鍵生成アルゴリズムにより生成された第2の鍵を用いて、前記第1の鍵のもとになる情報を暗号化した暗号化第1の鍵のもとになる情報と、

前記所定の鍵生成アルゴリズムを特定するためのアルゴリズム特定情報と、前記初期値を示す初期値情報と、を伝送することを特徴とするコンテンツ情報伝送方法。

【請求項2】第1の鍵のもとになる情報から生成された第1の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

与えられた初期値に基づき所定の鍵生成アルゴリズムにより生成された第2の鍵を用いて、前記第1の鍵のもとになる情報を暗号化した暗号化第1の鍵のもとになる情報と、

前記所定の鍵生成アルゴリズムを特定するためのアルゴリズム特定情報と、

前記初期値を示す初期値情報と、を記録することを特徴とするコンテンツ情報記録方法。

【請求項3】第1の鍵のもとになる情報から生成された第1の鍵を用いてコンテンツ情報を暗号化して暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段と、与えられた初期値に基づき所定の鍵生成アルゴリズムにより生成された第2の鍵を用いて、前記第1の鍵のもとになる情報を暗号化して暗号化第1の鍵のもとになる情報を出力する第1の鍵情報暗号化手段と、

前記暗号化コンテンツ情報、前記暗号化第1の鍵のもとになる情報、前記所定の鍵生成アルゴリズムを特定するためのアルゴリズム特定情報、及び前記初期値を示す初期値情報を伝送する伝送手段と、を備えたことを特徴とするコンテンツ情報伝送装置。

【請求項4】第1の鍵のもとになる情報から生成された第1の鍵を用いてコンテンツ情報を暗号化して暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段と、与えられた初期値に基づき所定の鍵生成アルゴリズムにより生成された第2の鍵を用いて、前記第1の鍵のもとになる情報を暗号化して暗号化第1の鍵のもとになる情報を出力する第1の鍵情報暗号化手段と、

前記暗号化コンテンツ情報、前記暗号化第1の鍵のもとになる情報、前記所定の鍵生成アルゴリズムを特定するためのアルゴリズム特定情報、及び前記初期値を示す初期値情報を媒体に記録する記録手段と、を備えたことを特徴とするコンテンツ情報記録装置。

【請求項5】第1の鍵のもとになる情報から生成された第1の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

与えられた初期値に基づき所定の鍵生成アルゴリズムに

より生成された第2の鍵を用いて、前記第1の鍵のもとになる情報を暗号化した暗号化第1の鍵のもとになる情報と、

前記所定の鍵生成アルゴリズムを特定するためのアルゴリズム特定情報と、

前記初期値を示す初期値情報と、を伝送することを特徴とする伝送媒体。

【請求項6】第1の鍵のもとになる情報から生成された第1の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

与えられた初期値に基づき所定の鍵生成アルゴリズムにより生成された第2の鍵を用いて、前記第1の鍵のもとになる情報を暗号化した暗号化第1の鍵のもとになる情報と、

前記所定の鍵生成アルゴリズムを特定するためのアルゴリズム特定情報と、

前記初期値を示す初期値情報と、を記録したことを特徴とする記録媒体。

【請求項7】前記第1の鍵情報暗号化手段は、与えられた初期値に基づき所定の鍵生成アルゴリズムにより第2の鍵を生成する鍵生成手段を備え、その鍵生成手段は特定の既約原始多項式を用いた線形フィードバックシフトレジスタを有することを特徴とする請求項3記載のコンテンツ情報伝送装置、または請求項4記載のコンテンツ情報記録装置。

【請求項8】第1の鍵のもとになる情報から生成された第1の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

与えられた初期値に基づき所定の鍵生成アルゴリズムにより生成された第2の鍵を用いて、前記第1の鍵のもとになる情報を部分的に暗号化した暗号化第1の鍵のもとになる情報と、

前記所定の鍵生成アルゴリズムを特定するためのアルゴリズム特定情報と、

前記初期値を示す初期値情報と、を伝送することを特徴とするコンテンツ情報伝送方法。

【請求項9】第1の鍵のもとになる情報から生成された第1の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

与えられた初期値に基づき所定の鍵生成アルゴリズムにより生成された第2の鍵を用いて、前記第1の鍵のもとになる情報を部分的に暗号化した暗号化第1の鍵のもとになる情報と、

前記所定の鍵生成アルゴリズムを特定するためのアルゴリズム特定情報と、

前記初期値を示す初期値情報と、を記録することを特徴とするコンテンツ情報記録方法。

【請求項10】第1の鍵のもとになる情報から生成された第1の鍵を用いてコンテンツ情報を暗号化して暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段

10

20

30

40

50

と、
与えられた初期値に基づき所定の鍵生成アルゴリズムにより生成された第2の鍵を用いて、前記第1の鍵のもとになる情報を部分的に暗号化して暗号化第1の鍵のもとになる情報を出力する第1の鍵情報暗号化手段と、
前記暗号化コンテンツ情報、前記暗号化第1の鍵のもとになる情報、前記所定の鍵生成アルゴリズムを特定するためのアルゴリズム特定情報、及び前記初期値を示す初期値情報を伝送する伝送手段と、を備えたことを特徴とするコンテンツ情報伝送装置。

【請求項11】第1の鍵のもとになる情報から生成された第1の鍵を用いてコンテンツ情報を暗号化して暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段と、

与えられた初期値に基づき所定の鍵生成アルゴリズムにより生成された第2の鍵を用いて、前記第1の鍵のもとになる情報を部分的に暗号化して暗号化第1の鍵のもとになる情報を出力する第1の鍵情報暗号化手段と、
前記暗号化コンテンツ情報、前記暗号化第1の鍵のもとになる情報、前記所定の鍵生成アルゴリズムを特定するためのアルゴリズム特定情報、及び前記初期値を示す初期値情報を媒体に記録する記録手段と、を備えたことを特徴とするコンテンツ情報記録装置。

【請求項12】第1の鍵のもとになる情報から生成された第1の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

与えられた初期値に基づき所定の鍵生成アルゴリズムにより生成された第2の鍵を用いて、前記第1の鍵のもとになる情報を部分的に暗号化した暗号化第1の鍵のもとになる情報と、

前記所定の鍵生成アルゴリズムを特定するためのアルゴリズム特定情報と、
前記初期値を示す初期値情報と、を伝送することを特徴とする伝送媒体。

【請求項13】第1の鍵のもとになる情報から生成された第1の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

与えられた初期値に基づき所定の鍵生成アルゴリズムにより生成された第2の鍵を用いて、前記第1の鍵のもとになる情報を部分的に暗号化した暗号化第1の鍵のもとになる情報と、

前記所定の鍵生成アルゴリズムを特定するためのアルゴリズム特定情報と、
前記初期値を示す初期値情報と、を記録したことを特徴とする記録媒体。

【請求項14】前記第1の鍵情報暗号化手段は、与えられた初期値に基づき所定の鍵生成アルゴリズムにより第2の鍵を生成する鍵生成手段を備え、その鍵生成手段は特定の既約原始多項式を用いた線形フィードバックシフトレジスタを有することを特徴とする請求項10記載の

コンテンツ情報伝送装置、または請求項11記載のコンテンツ情報記録装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンテンツ鍵とそのコンテンツ鍵を用いて暗号化された暗号化コンテンツ情報を伝送、記録するためのコンテンツ情報伝送方法、記録方法、伝送装置、記録装置、伝送媒体、及び記録媒体に関するものである。そして、この発明は特に、処理速度の点で有利な対称暗号化のみを用いた場合においても、コンテンツ情報の不正な再生（復号）、コピーをより強力に防止し著作権保護の強化を可能とするコンテンツ情報伝送方法、記録方法、伝送装置、記録装置、伝送媒体、及び記録媒体を提供することを目的としている。

【0002】

【従来の技術】暗号化技術の発展に伴い、ネットワークを利用してオーディオやビデオのデジタルデータを配信する有用な方法として、特開平10-269289のデジタルコンテンツ配布管理方法、デジタルコンテンツ再生方法及び装置がある。この発明では、デジタルコンテンツの配布側では、デジタルコンテンツを暗号化及び圧縮して加工し、この加工したデジタルコンテンツと暗号化したコンテンツ鍵、さらに暗号化した課金情報を通信相手側に送信する。そして、通信相手から送信されてきたコンテンツ使用情報に基づいて徴収した利用金を権利者に対して分配するようにしている。一方、デジタルコンテンツの再生側では、その加工されたデジタルコンテンツをコンテンツ鍵にて復号すると共に伸長して再生し、同時にコンテンツの使用に応じて課金情報の減額とコンテンツ使用情報を配布側に送信するようにし、記録されたコンテンツを持ち運びできるようにした。

【0003】また、特開平10-283268の情報記録媒体、記録装置、情報伝送システム、暗号解読装置では、暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とが記録されるものにおいて、上記暗号化鍵情報に、非暗号化された状態で上記暗号化情報を復号化する際の条件情報が追加記録される。即ち、暗号化鍵情報の制御情報内に、機器情報や領域情報が含まれているため、ユーザ側で暗号化された情報をそのままHDDや光ディスクにコピーして不正使用をすることを防止するようにしている。

【0004】暗号化方式は共通鍵を用いる対称暗号化方式と公開鍵、秘密鍵を用いる非対称暗号化方式に大別される。特開平10-283268に示されるように、オーディオやビデオ等の大容量のデジタルデータ（コンテンツ情報）を伝送する場合、コンテンツ情報については共通鍵（コンテンツ鍵）を設定し、処理速度の点で有利な対象暗号化を行うと共に、用いたコンテンツ鍵につ

いて別途非対称暗号化を行って伝送する方法がある。しかしながら非対称暗号化は主に処理速度の大きさが欠点として挙げられる。このため、暗号化装置と復号化装置に共通な上位の鍵、いわゆるマスター鍵を設定し、コンテンツ鍵をさらにマスター鍵を用いて対称暗号化し伝送する方法も良く用いられる。

【0005】

【発明が解決しようとする課題】しかしながら、上記の対称暗号化のみを用いる従来の方式では、暗号化装置を作成する側と復号化装置を作成する側において、暗号化方式に関する知識が一致してしまう。つまり、いずれの装置を作成する場合でもマスター鍵、コンテンツとコンテンツ鍵の暗号化アルゴリズムを知っていることが前提条件になると言うことである。このことは、暗号化装置を構成する知識で復号化装置を構成することが不可能ではないことを意味し、暗号化の目的である不正なコピーを防止し著作権を保護するという目的にそぐわない不正な復号化装置が流通する恐れがあった。

【0006】本発明は、処理速度の点で有利な対称暗号化のみを用いた場合においても、暗号化側に与えられる知識のみでは、復号化側において、指定された各アルゴリズム番号に従って暗号化に用いた鍵生成アルゴリズムをそれぞれ特定できないようにし、コンテンツ情報の不正な再生（復号）、コピーをより強力に防止し著作権保護の強化を可能とするコンテンツ情報伝送方法、記録方法、伝送装置、記録装置、伝送媒体、及び記録媒体を提供することを目的としている。

【0007】

【課題を解決するための手段】そこで、上記課題を解決するために本発明は、下記の方法・装置を提供するものである。

(1) 第1の鍵のもとになる情報から生成された第1の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、与えられた初期値に基づき所定の鍵生成アルゴリズムにより生成された第2の鍵を用いて、前記第1の鍵のもとになる情報を暗号化した暗号化第1の鍵のもとになる情報と、前記所定の鍵生成アルゴリズムを特定するためのアルゴリズム特定情報と、前記初期値を示す初期値情報と、を伝送することを特徴とするコンテンツ情報伝送方法。

(2) 第1の鍵のもとになる情報から生成された第1の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、与えられた初期値に基づき所定の鍵生成アルゴリズムにより生成された第2の鍵を用いて、前記第1の鍵のもとになる情報を暗号化した暗号化第1の鍵のもとになる情報と、前記所定の鍵生成アルゴリズムを特定するためのアルゴリズム特定情報と、前記初期値を示す初期値情報と、を記録することを特徴とするコンテンツ情報記録方法。

(3) 第1の鍵のもとになる情報から生成された第1

の鍵を用いてコンテンツ情報を暗号化して暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段と、与えられた初期値に基づき所定の鍵生成アルゴリズムにより生成された第2の鍵を用いて、前記第1の鍵のもとになる情報を暗号化して暗号化第1の鍵のもとになる情報を出力する第1の鍵情報暗号化手段と、前記暗号化コンテンツ情報、前記暗号化第1の鍵のもとになる情報、前記所定の鍵生成アルゴリズムを特定するためのアルゴリズム特定情報、及び前記初期値を示す初期値情報を伝送する伝送手段と、を備えたことを特徴とするコンテンツ情報伝送装置。

(4) 第1の鍵のもとになる情報から生成された第1の鍵を用いてコンテンツ情報を暗号化して暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段と、与えられた初期値に基づき所定の鍵生成アルゴリズムにより生成された第2の鍵を用いて、前記第1の鍵のもとになる情報を暗号化して暗号化第1の鍵のもとになる情報を出力する第1の鍵情報暗号化手段と、前記暗号化コンテンツ情報、前記暗号化第1の鍵のもとになる情報、前記所定の鍵生成アルゴリズムを特定するためのアルゴリズム特定情報、及び前記初期値を示す初期値情報を媒体に記録する記録手段と、を備えたことを特徴とするコンテンツ情報記録装置。

(5) 第1の鍵のもとになる情報から生成された第1の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、与えられた初期値に基づき所定の鍵生成アルゴリズムにより生成された第2の鍵を用いて、前記第1の鍵のもとになる情報を暗号化した暗号化第1の鍵のもとになる情報と、前記所定の鍵生成アルゴリズムを特定するためのアルゴリズム特定情報と、前記初期値を示す初期値情報と、を伝送することを特徴とする伝送媒体。

(6) 第1の鍵のもとになる情報から生成された第1の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、与えられた初期値に基づき所定の鍵生成アルゴリズムにより生成された第2の鍵を用いて、前記第1の鍵のもとになる情報を暗号化した暗号化第1の鍵のもとになる情報と、前記所定の鍵生成アルゴリズムを特定するためのアルゴリズム特定情報と、前記初期値を示す初期値情報と、を記録したことを特徴とする記録媒体。

(7) 前記第1の鍵情報暗号化手段は、与えられた初期値に基づき所定の鍵生成アルゴリズムにより第2の鍵を生成する鍵生成手段を備え、その鍵生成手段は特定の既約原始多項式を用いた線形フィードバックシフトレジスタを有することを特徴とする上記(3)記載のコンテンツ情報伝送装置、または上記(4)記載のコンテンツ情報記録装置。

【0008】

【発明の実施の形態】図1に本発明のコンテンツ情報記

録装置またはコンテンツ情報伝送装置の一実施例の概略構成を示す。なお、本説明においては、磁気記録媒体、光記録媒体、半導体メモリ等を記録媒体と呼び、光ケーブル、電線、無線伝送路等の信号を伝送する伝送媒体を伝送路と呼ぶこととする。

【0009】まず、記録側または送信側について説明する。記録側または送信側においては、第2の鍵を生成するための鍵生成ブロック1、第1の鍵（コンテンツ鍵）のもとになる情報を前記第2の鍵により暗号化する暗号化ブロック2、及び、第1の鍵（コンテンツ鍵）のもとになる情報から第1の鍵（コンテンツ鍵）を生成してコンテンツ情報の暗号化を行う暗号化ブロック3を備えている。

【0010】記録側または送信側の装置への入力は、
・再生側または受信側において第2の鍵生成のための鍵生成アルゴリズムの指定に用いられる、鍵生成ブロック1内で用いられる鍵生成アルゴリズムに対応したアルゴリズム番号と、
・鍵生成ブロック1に与えられる初期値と、
・コンテンツ情報の暗号化に用いられる第1の鍵（コンテンツ鍵）を生成するための第1の鍵のもとになる情報と、
・コンテンツ情報と、である。

【0011】鍵生成ブロック1の出力である第2の鍵は、第1の鍵（コンテンツ鍵）のもとになる情報を暗号化するための上位鍵の役割を果たし、ランダムかつ初期値によって大きく変化することが求められる。

【0012】図2に鍵生成ブロック1の一実施例を示す。この実施例においては、所定のビット数N（図例においてN=8）であるシフトレジスタ（r1～r8）と所定のレジスタ位置からの排他的論理和を得るためのゲート群（g1～g8）、係数設定バス及び初期値設定バスから構成されている。排他的論理和の結果を最下位レジスタへセットするこのような回路はリニアフィードバックシフトレジスタ（LFSR）と呼ばれている。初期値入力から初期値バスを通じて各レジスタにセットされると共に、係数入力によって各ゲートのスイッチ状態がセットされる。この後にシフトレジスタにクロックを与え、最上位レジスタからの出力を得る。

【0013】最も効果的にランダムな出力を得るためには設定係数がN次の原始多項式に対応していることが必要である。例えばN=8においては8次の原始多項式の1つである、

【0014】

【数1】

数1

$$x^8 + x^7 + x^2 + x + 1$$

【0015】を用いた場合、(g8, g7, g6, g5, g

4, g3, g2, g1)に対応して係数(1, 1, 0, 0, 0, 0, 1, 1)が各ゲートに入力される。さらに初期値設定は値0以外が選択される。最上位レジスタからの出力はM系列と呼ばれる、高いランダム性を有したビット列となるが、LFSRの性質上将来の出力に関する予測が容易であるので、乗算等の非線形性を有した関数による変換を出力に備えることが理想的である。この出力ビット列を所定のフォーマットで第1の鍵（コンテンツ鍵）のもとになる情報の暗号化に用いる。

10 【0016】第1の鍵のもとになる情報の暗号化ブロック2、及びコンテンツ情報の暗号化ブロック3については、DES等の広く公知である暗号化アルゴリズムを用いることができる。なお、暗号化された第1の鍵のもとになる情報は、第1の鍵のもとになる情報が第2の鍵により全て暗号化されたものでもよいし、部分的に暗号化されたものでもよい。（例えば、暗号化された第1の鍵のもとになる情報は、第1の鍵のもとになる情報の内の特に重要な部分のみが暗号化され、他の部分は暗号化されていない状態のものでもよい。）

20 【0017】記録媒体あるいは伝送路上へは、第2の鍵生成のための鍵生成アルゴリズムの指定に用いられるアルゴリズム番号、初期値、暗号化された第1の鍵のもとになる情報、暗号化されたコンテンツ情報が所定のフォーマットで記録あるいは伝送される。アルゴリズム番号は前記した特定の原始多項式に対して一意でなければならない。

【0018】なお、初期値やアルゴリズム番号は所定の関数により変換されて記録あるいは伝送されるようにしてもよい。（再生側または受信側では所定関数の逆関数を用いて初期値やアルゴリズム番号を得る。）

30 【0019】次に、再生側または受信側について説明する。復号化装置は、第2の鍵生成のための鍵生成アルゴリズムを特定するための参照テーブル4、第2の鍵生成のための鍵生成ブロック5、第1の鍵（コンテンツ鍵）のもとになる情報の復号化ブロック6、及び、復号された第1の鍵のもとになる情報から第1の鍵（コンテンツ鍵）を生成してコンテンツ情報を復号するの復号化ブロック7を備えている。鍵生成ブロック5は記録側または送信側装置におけるものと同様の構成とする。第1の鍵（コンテンツ鍵）のもとになる情報の復号化ブロック6、及びコンテンツ情報の復号化ブロック7については、記録側または送信側装置の暗号化ブロック2及び3とそれぞれ対を成す構成とする。

40 【0020】参照テーブル4は、アルゴリズム番号から第2の鍵生成のための原始多項式を特定するために設けられている。参照テーブル4は具体的にはROMで実現され、アルゴリズム番号を入力アドレスとして原始多項式に対応した係数列を出力として得るものである。原始多項式を8次とした場合の参照テーブルの構成例を表1に示す。復号化装置の動作を以下に説明する。

【0021】

【表1】

表1 参照テーブルの一例

アルゴリズム番号	係数列	原始多項式
0	(1, 1, 0, 0, 0, 0, 1, 1)	$x^8 + x^7 + x^2 + x + 1$
1	(1, 0, 0, 0, 1, 1, 1, 0)	$x^8 + x^4 + x^3 + x^2 + 1$
2	(1, 0, 1, 1, 0, 1, 0, 0)	$x^8 + x^6 + x^5 + x^3 + 1$
3	(1, 1, 1, 1, 0, 0, 1, 1)	$x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$
4	(1, 0, 0, 1, 0, 1, 0, 1)	$x^8 + x^5 + x^3 + x + 1$
5	(1, 0, 1, 1, 0, 0, 1, 0)	$x^8 + x^6 + x^5 + x^2 + 1$
6	(1, 0, 1, 1, 0, 0, 0, 1)	$x^8 + x^6 + x^5 + x + 1$
7	(1, 0, 1, 0, 1, 1, 1, 1)	$x^8 + x^6 + x^4 + x^3 + x^2 + x + 1$

【0022】復号化装置は、記録媒体あるいは伝送路からのアルゴリズム番号を参照テーブル4へ入力し、対応する係数列を得る。この係数列と記録媒体あるいは伝送路からの初期値を鍵生成ブロック5へ入力し、記録側または送信側と同様にレジスタへの初期値のセットとゲート状態のセットを行った後にクロックを与えて出力のビット列を得る。出力ビット列は所定のフォーマットで第1の鍵（コンテンツ鍵）のもとになる情報の復号化鍵として用いられ、復号化ブロック6において記録媒体あるいは伝送路からの情報を第1の鍵（コンテンツ鍵）のもとになる情報へ復号化する。さらに、この復号された第1の鍵のもとになる情報から第1の鍵（コンテンツ鍵）を生成して、記録媒体あるいは伝送路からの暗号化コンテンツ情報を復号化ブロック7において復号化する。

【0023】実施にあたっては、暗号化強度保持の観点から復号化装置全体が解析等を受け難いように実現されることが望ましい。特に、参照テーブル4は復号化装置の外部に内容が読み出される可能性が低くなるような配慮が必要である。好適な実施方法としては復号化装置全体を一体のLSIとすることである。

【0024】このように、本実施例では、参照テーブル4が復号化側のみに与えられるため、暗号化側に与えられる知識のみでは指定されたアルゴリズム番号に従って鍵生成アルゴリズムを変更する機能を持った復号化装置を作成することが不可能である。よって、懸念される不正な復号化装置が作成されることを防止する効果がある。さらに、暗号化段階で用いられている鍵生成アルゴリズムのみを実現している不正な復号化装置が発見された場合、暗号化側で鍵生成アルゴリズムを変更すると同時に伝送するアルゴリズム番号を変更することで、不正

な復号化装置での復号化が不可能なコンテンツの配信、配布を可能とする。

【0025】なお、上記実施例の記録または伝送装置、及び復号化装置においては、第1の鍵（コンテンツ鍵）のもとになる情報と鍵生成ブロックが出力する上位鍵（第2の鍵）を用いると共に暗号化、復号化ブロックが2段となっている例を示したが、第1の鍵（コンテンツ鍵）のもとになる情報をM個用意し、第1の鍵（コンテンツ鍵）のもとになる情報の暗号化をM段としてもよい。この場合は媒体または伝送路上で、M個の暗号化第1の鍵のもとになる情報が記録、伝送されることになる。

【0026】

【発明の効果】以上のように、本発明によれば、処理速度の点で有利な対称暗号化のみを用いた場合においても、暗号化側に与えられる知識のみでは、復号化側において、指定された各アルゴリズム番号に従って暗号化に用いた鍵生成アルゴリズムをそれぞれ特定できないようにすることにより、コンテンツ情報の不正な再生（復号）、コピーをより強力に防止し著作権保護の強化を可能とする。

【図面の簡単な説明】

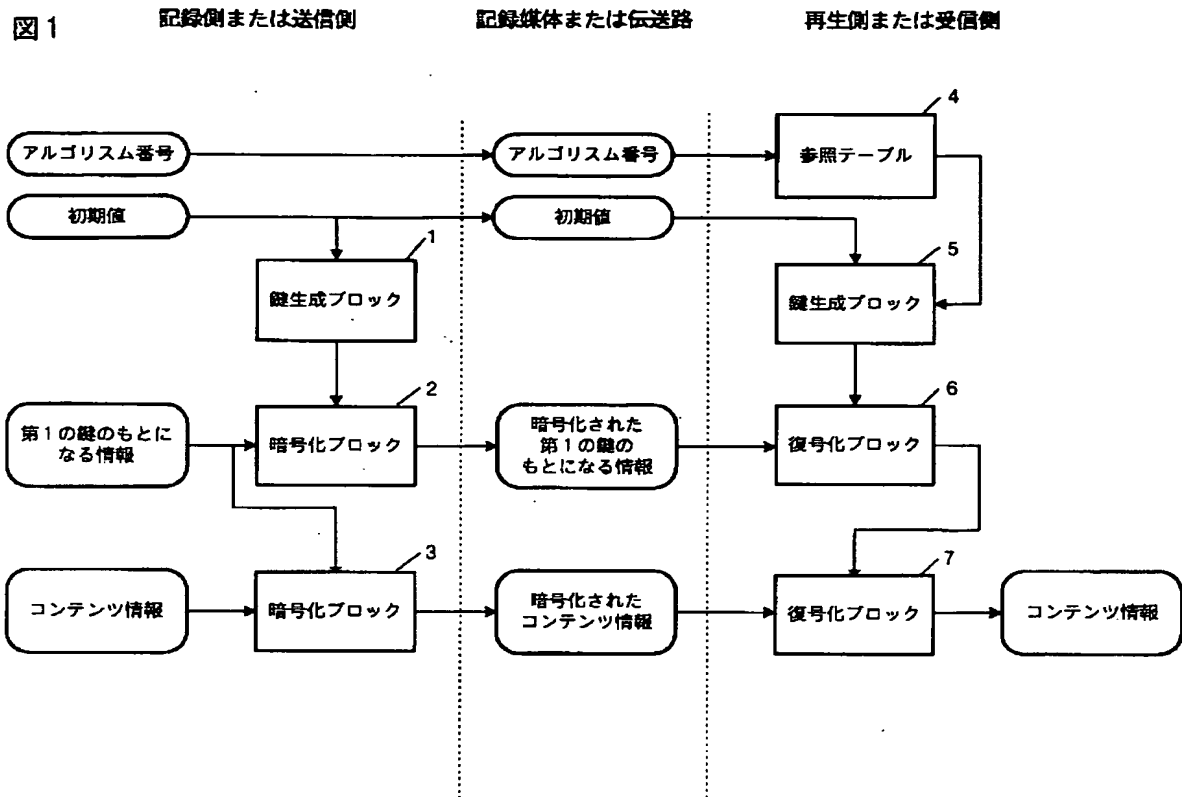
【図1】本発明の一実施例の概略構成を示す図である。

【図2】記録側または送信側の鍵生成ブロックの一例を示す図である。

【符号の説明】

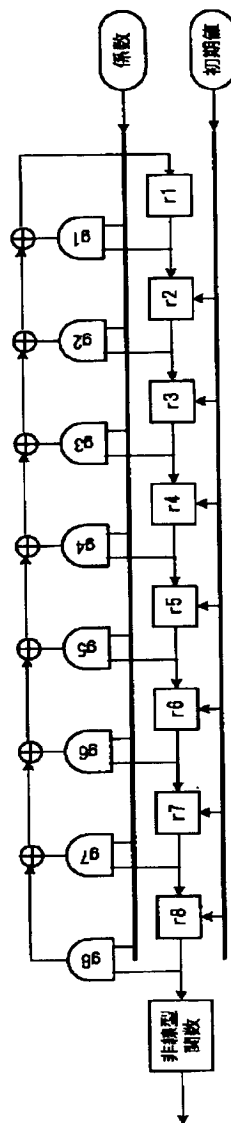
- 1, 5 鍵生成ブロック
- 2, 3 暗号化ブロック
- 4 参照テーブル
- 6, 7 復号化ブロック

【図1】



【図 2】

図 2 鍵生成ブロックの実施例



フロントページの続き

(72) 発明者 上田 健二郎
 神奈川県横浜市神奈川区守屋町 3 丁目 12 番
 地 日本ビクター株式会社内
 (72) 発明者 日暮 誠司
 神奈川県横浜市神奈川区守屋町 3 丁目 12 番
 地 日本ビクター株式会社内

F ターム(参考) 5B085 AE13 AE29
 5J104 AA07 AA16 CA02 DA04 EA06
 JA03 JA13 KA04 NA02 NA08
 NA23 NA37 PA07 PA14
 9A001 BB03 BB05 CC05 CC07 EE03
 GG01 KK31 LL03